PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-222063
(43)Date of publication of application : 21.08.1998

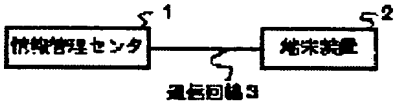
(51)Int.Cl. G09C 1/00
G06F 15/00
H04L 9/32

(21)Application number : 09-035474
(22)Date of filing : 04.02.1997

(71)Applicant : VICTOR CO OF JAPAN LTD
(72)Inventor : SHISHIDO ICHIRO

(54) DIGITAL INFORMATION MANAGEMENT SYSTEM, TERMINAL DEVICE, INFORMATION MANAGEMENT CENTER, AND METHOD OF CONTROLLING DIGITAL INFORMATION

(57)Abstract:
PROBLEM TO BE SOLVED: To make it possible to prevent illegal copy without losing convenience for proper users.
SOLUTION: When digital information is used, a registration number and a registration number authentication corresponding to the digital information used from a terminal equipment 2 are transmitted to an information management center 1. The information management center 1 examines a validity of the received registration number and also checks the conditions for the use of the corresponding digital information, and transmits data indicating a permission for the use if the number has a validity, and transmits data for inhibiting the use to terminal device 2, if the number is not duly permitted for the use. The terminal device 2 is arranged so that the digital information is usable thereon only when it receives a permission for the use.



LEGAL STATUS

[Date of request for examination] 17.03.2000
[Date of sending the examiner's decision of rejection] 17.10.2003
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平10－222063

(43)公開日　平成10年(1998)８月21日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０９Ｃ　1/00	６４０	Ｇ０９Ｃ　1/00	６４０Ｂ
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｚ
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７５Ｄ
			６７５Ｂ

審査請求　未請求　請求項の数７　ＦＤ　（全 10 頁）

(21)出願番号　特願平9－35474

(22)出願日　平成９年(1997)２月４日

(71)出願人　000004329
日本ビクター株式会社
神奈川県横浜市神奈川区守屋町３丁目12番地

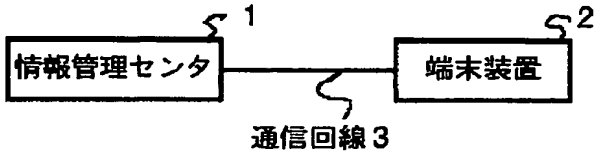
(72)発明者　宍戸　一郎
神奈川県横浜市神奈川区守屋町３丁目12番地　日本ビクター株式会社内

(54)【発明の名称】　デジタル情報管理システム、端末装置、情報管理センタ及びデジタル情報管理方法

(57)【要約】

【課題】　正当な利用者の利便性を損なうことなく、不正コピーを防止することができなかった。

【解決手段】　デジタル情報を使用する際に、端末装置２から使用するデジタル情報に対応する登録番号と登録番号認証子とを情報管理センタ１に送信する。情報管理センタ１では受信した登録番号の正当性を検査すると共に該当するデジタル情報の使用条件を確認し、正当に使用可能な状態であれば使用許可を示すデータを端末装置２に送信し、正当に使用することができない状態であれば使用禁止を示すデータを端末装置２に送信する。端末装置２では使用許可を示すデータを受信した時のみデジタル情報を使用できるようにする。



1

【特許請求の範囲】

【請求項１】端末装置と情報管理センタとが通信回線を介して接続され、前記端末装置に記憶されているデジタル情報の管理を行うデジタル情報管理システムであって、

前記端末装置は、前記情報管理センタとの通信を行う第１の通信手段と、前記デジタル情報を識別する登録番号と登録番号認証子と前記デジタル情報本体とを格納するデジタル情報格納手段と、前記デジタル情報の利用手順を制御する第１の制御手段とで構成され、

前記情報管理センタは、前記端末装置との通信を行う第２の通信手段と、前記登録番号とその使用条件を記憶格納する使用条件格納手段と、前記認証子を使って前記登録番号を認証する認証処理手段と、前記情報管理センタ全体を制御する第２の制御手段とで構成されることを特徴とするデジタル情報管理システム。

【請求項２】情報管理センタとの通信を行う通信手段と、デジタル情報を識別する登録番号と登録番号認証子とデジタル情報本体とを格納するデジタル情報格納手段と、前記デジタル情報の利用手順を制御する制御手段とで構成されたことを特徴とする端末装置。

【請求項３】前記登録番号あるいは前記登録番号の認証子の特定の部分のビット列と前記デジタル情報本体の特定の部分のビット列が一致するように前記登録番号が設定されており、前記デジタル情報格納手段において前記一致するビット列を重ね合わせて配置することを特徴とする請求項２記載の端末装置。

【請求項４】端末装置との通信を行う通信手段と、登録番号とその使用条件を記憶格納する使用条件格納手段と、前記認証子を使って前記登録番号を認証する認証処理手段と、前記各手段を制御する制御手段とで構成されたことを特徴とする情報管理センタ。

【請求項５】前記登録番号あるいは前記登録番号の認証子の特定の部分のビット列と前記デジタル情報本体の特定の部分のビット列が一致するように前記登録番号を設定することを特徴とする請求項４記載の情報管理センタ。

【請求項６】端末装置に記憶されているデジタル情報の管理を行うデジタル情報管理方法であって、

前記端末装置から前記デジタル情報を識別する登録番号と登録番号認証子とを通信回線を介して接続されている情報管理センタに送信する第１の手順と、

前記情報管理センタにて受信した前記登録番号の正当性を前記登録番号認証子と暗号鍵を用いて確認する第２の手順と、

前記情報管理センタにて受信した前記登録番号に該当する前記デジタル情報が前記使用条件に合致しているかを確認する第３の手順と、

前記情報管理センタにて前記使用条件に合致していれば、使用許可を示すデータを前記端末装置に送信し、前記使用条件に合致していなければ、使用禁止を示すデータを前記端末装置に送信する第４の手順と、

前記端末装置にて使用許可を示すデータを受信したときのみ前記デジタル情報を使用できるようにする第５の手順とからなることを特徴とするデジタル情報管理方法。

【請求項７】前記登録番号認証子として、前記登録番号あるいは前記登録番号を一方向性ハッシュ関数に代入した値を前記情報管理センタの暗号鍵で暗号化した値を用いたことを特徴とする請求項６記載のデジタル情報管理方法。

2

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、端末装置内に蓄積されたデジタル情報の不正利用を防止するデジタル情報管理システム及びにデジタル情報管理方法に係り、特に規定回数や規定期間を越えた場合などを含む不正利用者に対してデジタル情報を利用できないようにするデジタル情報管理システム及びにデジタル情報管理方法に関するものである。

【０００２】

【従来の技術】近年、テキスト、音声、静止画、動画等をデジタル化して、コンピュータ上で利用することが急激に増えている。しかしデジタルデータには、コンピュータ上で元データと全く同じものを容易にコピー／作成できるという性質があるので、不正コピーにより著作権者やデータ販売者の権利が侵害されるといった問題が生じている。

【０００３】また最近では、単に不正コピーを防止するだけでなく、データの有用性を理解してもらうために使用回数や使用期間を限定してデータを利用させたり、デジタル動画等を再生する回数に応じて料金を徴収したりしたいというニーズも高まっている。これらの問題解決やニーズを実現する方法としては、例えば特開平3-288227号が開示されている。これはソフトウェアの使用回数を制限する方法であり、簡単に説明すると、まず、ソフトウェアの提供者が通信手段を介して使用制限回数と使用回数の初期値を利用者のコンピュータ（端末装置）に送出し、それらを利用者のコンピュータ内の記録媒体に記録しておく。そして、ソフトウェア実行時に使用回数を更新すると共に使用制限回数と比較して、使用回数が使用制限回数を越えた場合にソフトウェアの実行を中止するという方法である。

【０００４】しかしこの方法では、利用者のコンピュータ内で使用回数と使用制限回数を記録管理しているので、専用のコンピュータならともかく、一般に仕様が公開されているハードウェアやオペレーティングシステムを使用した、いわゆる一般的なコンピュータ（パーソナルコンピュータ）では、技術レベルの高い利用者が使用回数や使用制限回数を書き換える可能性がある。また、ソフトウェア提供者に対して利用するコンピュータの電

話番号やアドレスを教える必要があるので、手続きの煩雑さやプライバシー保護の点で問題があった。

【０００５】また、別の方法が特開平7-131452号に開示されている。これは、端末装置から通信回線を介して情報センタに蓄積されているデジタル情報をダウンロードする際に、その端末装置でのみデジタル情報が利用出来るようにデジタル情報を暗号化すると共に、そのデジタル情報の利用条件をダウンロードし、端末装置内の機密処理部に格納する。そして、情報を利用する際に機密処理部に格納されている決められた使用条件に合うかどうかチェックし、この条件に合わない場合は利用を禁止するという方法である。

【０００６】

【発明が解決しようとする課題】この後者の方法では、端末装置内で暗号の共通鍵、使用条件、使用履歴等を格納するための機密処理部が利用者から完全に隠蔽されることが必要となるが、より多くの利用者を獲得する為には、端末装置は一般的な構成のコンピュータ（パーソナルコンピュータ）であることが望ましい。しかし、利用者が不正な方法でも読み書きすることができない耐タンパー性を持つ特殊な装置を付加することなく、ごく一般的な構成のコンピュータでこのような機密処理部を実現することは非常に困難であった。また、特殊な装置を使用すると、端末装置のコストが高くなったり、利用者数が限定されてしまい、実用上問題があった。

【０００７】さらに、上記２つの方法では、購入したソフトウェアやデジタル情報を利用出来る端末装置がダウンロードした端末装置1台だけに限定されてしまうので、例えば、正当にデジタル情報を購入した利用者が自宅と職場の両方でそのデジタル情報を利用したいとしても、端末装置を持ち運んで移動させなければそのように利用することは不可能であり、正当な利用者の利便性を損なう恐れがあった。また別の方法として、デジタル情報を利用する際に、その都度サーバからダウンロードを行い、端末装置内にデジタル情報を蓄積させないことによって不正コピーを防止する方法も考えられるが、通信コストが高くなり、ダウンロードにも時間がかかるといった問題があった。

【０００８】そこで本発明は、正当な利用者の利便性を損なうことなく、不正コピーを防止し、また、使用回数や使用期間を限定してデータを利用させたり、デジタル動画等を再生する回数に応じて料金を徴収したりすることのできるデジタル情報管理システムを提供することを目的とする。

【０００９】

【課題を解決するための手段】上記目的を達成するための手段として、以下に示すデジタル情報管理システム、端末装置、情報管理センタ及びデジタル情報管理方法を提供しようとするものである。

【００１０】１．端末装置と情報管理センタとが通信回線を介して接続され、前記端末装置に記憶されているデジタル情報の管理を行うデジタル情報管理システムであって、前記端末装置は、前記情報管理センタとの通信を行う第１の通信手段と、前記デジタル情報を識別する登録番号と登録番号認証子と前記デジタル情報本体とを格納するデジタル情報格納手段と、前記デジタル情報の利用手順を制御する第１の制御手段とで構成され、前記情報管理センタは、前記端末装置との通信を行う第２の通信手段と、前記登録番号とその使用条件を記憶格納する使用条件格納手段と、前記認証子を使って前記登録番号を認証する認証処理手段と、前記情報管理センタ全体を制御する第２の制御手段とで構成されることを特徴とするデジタル情報管理システム。

【００１１】２．情報管理センタとの通信を行う通信手段と、デジタル情報を識別する登録番号と登録番号認証子とデジタル情報本体とを格納するデジタル情報格納手段と、前記デジタル情報の利用手順を制御する制御手段とで構成されたことを特徴とする端末装置。

【００１２】３．前記登録番号あるいは前記登録番号の認証子の特定の部分のビット列と前記デジタル情報本体の特定の部分のビット列が一致するように前記登録番号が設定されており、前記デジタル情報格納手段において前記一致するビット列を重ね合わせて配置することを特徴とする上記２．記載の端末装置。

【００１３】４．端末装置との通信を行う通信手段と、登録番号とその使用条件を記憶格納する使用条件格納手段と、前記認証子を使って前記登録番号を認証する認証処理手段と、前記各手段を制御する制御手段とで構成されたことを特徴とする情報管理センタ。

【００１４】５．前記登録番号あるいは前記登録番号の認証子の特定の部分のビット列と前記デジタル情報本体の特定の部分のビット列が一致するように前記登録番号を設定することを特徴とする上記４．記載の情報管理センタ。

【００１５】６．端末装置に記憶されているデジタル情報の管理を行うデジタル情報管理方法であって、前記端末装置から前記デジタル情報を識別する登録番号と登録番号認証子とを通信回線を介して接続されている情報管理センタに送信する第１の手順と、前記情報管理センタにて受信した前記登録番号の正当性を前記登録番号認証子と暗号鍵を用いて確認する第２の手順と、前記情報管理センタにて受信した前記登録番号に該当する前記デジタル情報が前記使用条件に合致しているかを確認する第３の手順と、前記情報管理センタにて前記使用条件に合致していれば、使用許可を示すデータを前記端末装置に送信し、前記使用条件に合致していなければ、使用禁止を示すデータを前記端末装置に送信する第４の手順と、前記端末装置にて使用許可を示すデータを受信したときのみ前記デジタル情報を使用できるようにする第５の手順とからなることを特徴とするデジタル情報管理方法。

【００１６】７．前記登録番号認証子として、前記登録番号あるいは前記登録番号を一方向性ハッシュ関数に代入した値を前記情報管理センタの暗号鍵で暗号化した値を用いたことを特徴とする上記６記載のデジタル情報管理方法。

【００１７】

【発明の実施の形態】本発明のデジタル情報管理システムは、図１に示すように端末装置２と情報管理センタ１とが通信回線３を介して接続されているシステムであり、情報管理センタ１においてデジタル情報の使用条件及び使用状況を記録管理することが本発明の特徴である。そして、端末装置２は、図２に示すように、情報管理センタ１との通信を行う通信手段（第１の通信手段）４と、デジタル情報を一意に識別可能な登録番号と登録番号の認証子とデジタル情報本体とを格納するデジタル情報格納手段６と、デジタル情報の利用手順を制御する制御手段（第１の制御手段）５と、入力手段８及び出力手段９を有している。

【００１８】また、情報管理センタ１は、図３に示すように、端末装置２との通信を行う通信手段（第２の通信手段）１０１と、登録番号とその使用条件を記憶格納する使用条件格納手段１０３と、登録番号の認証をおこなう認証処理手段１０４と、制御手段（第２の制御手段）１０２とを有している。このような構成のデジタル情報管理システムにおいて、実際にデジタル情報を管理するデジタル情報管理方法について説明する。

【００１９】まず、情報販売者は、またはデジタル情報を販売する際に、登録番号と登録番号の認証子をデジタル情報本体に付加すると共に、登録番号とその使用条件を情報管理センタ１の使用条件格納手段１０３に登録する。ここで、登録番号と登録番号の認証子をデジタル情報本体に付加する方法としては、例えば、デジタル情報があらかじめインストールされていたり、ＣＤ－ＲＯＭなどの可搬型の記録媒体により供給されていて、デジタル情報が既に端末装置２のデジタル情報格納手段６に格納されている場合には、利用者として登録する際に登録番号と登録番号の認証子を端末装置２に対して通信回線３を介して供給し、デジタル情報を通信回線３を介してダウンロードする場合は、デジタル情報と共に供給すれば良い。

【００２０】そして、登録後、利用者が端末装置２でデジタル情報を使用するために、端末装置２の制御手段５に使用する旨の指示を与えると、端末装置２と情報管理センタ１との間で以下の処理が行なわれた後、デジタル情報が利用可能となる。まず端末装置２は、登録番号と登録番号の認証子を情報管理センタ１に送信する。情報管理センタ１では受信した登録番号に該当するデジタル情報の使用条件を確認し、正当に使用可能な状態であるかを確認する。正当な使用であれば使用許可を示すデータを端末装置２に送信する。もし、正当な使用でなければ使用禁止を示すデータを端末装置２に送信する。端末装置２では情報管理センタ１から受信したデータが使用許可を示す時のみデジタル情報を使用できるように制御する。

【００２１】このような方法を用いることにより、利用者が不正に使用条件を変えることが困難になるので、デジタル情報の使用回数や使用期限を正確に管理することができる。また、本発明における端末装置２は、複雑な処理が必要となる暗号処理部が不要である。また機密保持が必要な共通鍵や秘密鍵を格納していない。さらに利用者から隠蔽する必要のある使用条件や使用履歴を格納していないので、従来例のような機密処理部を必要としない。従って、特殊な装置を付加しない一般的な構成のコンピュータを端末装置２として使った場合でも、デジタル情報の使用回数や使用期限を正確に管理することが可能になる。

【００２２】

【実施例】本発明デジタル情報管理システムの一実施例を図面と共に説明する。図１は本実施例の全体の構成を示す図である。同図において、デジタル情報を利用する端末装置２とデジタル情報の使用条件を管理する情報管理センタ１とが、電話回線、専用線、LAN等の通信回線３によって接続されている。そして、この端末装置２の構成例を図２に示す。なお、パーソナルコンピュータで構成した場合には、同図中、点線で示した部分がパソコン本体となり、それに、キーボードやマウスなどの入力手段８及びディスプレイなどの出力手段９が接続されている。点線で囲まれたパソコン本体には、情報管理センタ１との通信を行う通信手段４と、デジタル情報を一意に識別可能な登録番号と登録番号の認証子とデジタル情報本体とを格納するデジタル情報格納手段６と、デジタル情報の利用手順を制御する制御手段５とを有している。

【００２３】この通信手段４は、通信回線３の種類に応じてモデムやＬＡＮコントローラ等で構成されており、制御手段５の指示により情報管理センタ１との通信を行うものである。デジタル情報格納手段６は、ハードディスク、フロッピーディスク、MOディスク、あるいはその他の不揮発性メモリ等で構成されている。そして、1つのデジタル情報につき、デジタル情報を識別するための登録番号と登録番号の認証子とデジタル情報本体とが格納される。

【００２４】制御手段５は、CPU、RAM、ROM等で構成されており、デジタル情報を利用者が利用する際に、決められた手順に従って端末装置２の各部を制御するものである。入力手段８は、キーボード、マウス、操作ボタン、リモコン等で構成されており、利用者が利用するデジタル情報や利用方法を選択した結果の指示を制御手段５に与える為に使用するものである。情報出力手段９は、ディスプレイ、スピーカ、プリンタ等の出力装置で

あり、デジタル情報の種類に応じて、例えば静止画や動画ならばディスプレイ、音声ならばスピーカといったように適切な出力装置が選択される。

【００２５】そして、図３に情報管理センタ１の構成を示す。この情報管理センタ１は、端末装置２との通信を行う通信手段１０１と、使用条件を記憶格納する使用条件格納手段１０３と、登録番号の認証をおこなう認証処理手段１０４と、制御手段１０２とで構成されている。

【００２６】使用条件格納手段１０３には、図４に示す形式の使用条件テーブルが格納されている。図４に示すテーブルにおいて、登録番号は情報管理センタ１で管理するデジタル情報を一意に識別する番号である。この登録番号は端末装置２のデジタル情報格納手段６に格納されている登録番号と同じものである。なお後述するように、登録番号の一部のビット列がデジタル情報本体の一部のビット列と一致するように登録番号を割り当てても良い。また、期間制限フラグは使用期間の制限を行うかどうかを示すフラグであり、使用期間の制限を行う場合は「1」に、行わない場合は「0」に設定されている。回数制限フラグは使用回数の制限を行うかどうかを示すフラグであり、使用回数の制限を行う場合は「1」に、行わない場合は「0」に設定されている。許可開始日時は期間制限フラグが「1」の場合に有効であり、使用許可を開始する年、月日、時刻を示している。許可終了日時は期間制限フラグが「1」の場合に有効であり、使用許可を終了する年、月日、時刻を示している。使用可能回数は回数制限フラグが「1」の場合に有効であり、今後使用可能な回数を示している。したがって、回数制限フラグが「1」であって、このフィールドが「0」になると使用出来なくなる。そして、使用期間と使用回数を両方制限する場合は、2つのフラグを両方「1」にする。

【００２７】このような構成のデジタル情報管理システムにおいて、デジタル情報販売者は、デジタル情報のダウンロードなどによって利用者にデジタル情報を販売する際や、ＣＤ－ＲＯＭ等の可搬型の記録媒体やプレインストールによりデジタル情報を既に手に入れている利用者を登録する際に、図示しない入力手段や管理用端末を介して情報管理センタ１の制御手段１０２に所定の指示を与え、図５に示すフローチャートの手順に従って使用条件格納手段１０３に格納されている使用条件テーブルの設定を行う。

【００２８】まず、使用条件テーブルの登録番号に使われていない番号を1つ選び新しい登録番号Nとする(ステップS11)。次に、販売するデジタル情報本体に登録番号Nを付加する(ステップS12)。これについては後ほど詳しく述べる。次に、使用条件テーブルの新たなエントリに登録番号Nを書き込む(ステップS13)。そして、デジタル情報の内容や利用者との契約により、各種の利用制限の設定を行う。まず、使用期間を制限する場合は（ステップS14→YES）、期間制限フラグを「1」にセットし、許可開始時間と許可終了時間を各々許可開始日時フィールド、許可終了日時フィールドに設定する(ステップS15)。許可開始時間あるいは許可終了時間のどちらか一方を設定する必要がない場合は、そのフィールドを所定の初期値（例えば０）にしておく。使用期間を制限しない場合は（ステップS14→NO）、期間制限フラグを「0」にセットし、許可開始時間と許可終了時間を各々所定の初期値（例えば０）に設定する(ステップS16)。

【００２９】使用期間の設定後はステップ17の使用回数の設定に移行する。そして、使用回数を制限する場合は（ステップS17→YES）、回数制限フラグを「1」にセットすると共に、使用可能回数フィールドを設定する(ステップS18)。例えば、3回だけ使用を許可する場合は、このフィールドを「3」とする。使用回数を制限しない場合は（ステップS17→NO）、回数制限フラグを「0」にセットすると共に、使用可能回数フィールドを所定の初期値（例えば０）にする(ステップS19)。以上で使用条件テーブルの設定が終了する。

【００３０】さらに、デジタル情報販売者は、図示しない入力手段や管理用端末を介して情報管理センタ１の制御手段１０２に所定の指示を与え、端末装置２に供給する配布データを作成する。この配布データのフォーマットの例を図６（A），(B)，(C)，(D)に示す。同図中の登録番号認証子５２は情報管理センタ１の認証処理手段１０４にて作成される。なお、同図に示す配布データは、デジタル情報本体５４も一緒に通信回線３または可搬型の記録媒体を介して供給する場合のフォーマットであり、既に、デジタル情報本体５４が端末装置２に供給されている場合には、同図に示すフォーマットからデジタル情報本体５４を省略した形で作成して端末装置２に供給し、端末装置２内で図６に示すフォーマットに作成し直す。

【００３１】図６(A)に示すフォーマットは、基本的なフォーマットであり、ビット長Ｐのフォーマット種別５１、ビット長Ｑの登録番号認証子５２、ビット長Ｓの登録番号５３、ビット長Ｕの情報本体５４が並んだ形式となっている。図６(B)に示すフォーマットは、登録番号５３の最後のVビットと情報本体５４の最初のＶビットが一致しており、共通ビットを重ね合わせて端末装置２のデジタル情報格納手段６に格納するものである。同様に同図(C)に示すフォーマットは、登録番号５３の最初のＶビットと情報本体５４の最後のＶビットが一致しており、共通ビットを重ね合わせて端末装置２のデジタル情報格納手段６に格納するものである。同様に同図(D)に示すフォーマットは、登録番号認証子５２の最後のVビットと情報本体５４の最初のＶビットが一致しており、共通ビットを重ね合わせて端末装置２のデジタル情報格納手段６に格納したものである。

【００３２】そして、これら図６（B），(C)，(D)に示すフォーマットとした場合には、端末装置２側で登録番

号５３や登録番号認証子５２を他のデジタル情報の登録番号や登録番号認証子に置き換えると、情報本体の一部のデータも書きかわり、正常に情報本体５４を利用することができなくなる。従ってこのような不正行為を抑止することができる。また、重ねあわせた分、デジタル情報格納手段６のメモリ容量を小さくすることができる。なお、図６の（B），(C)，(D)は一例であり、登録番号あるいは登録番号認証子の一部のビット列と情報本体の一部のビット列を重ね合わせた他のフォーマットを使用しても良い。以下では、このようなフォーマットの代表として同図(B)を例にとって説明する。

【００３３】図６に示す配布データにおいて、フォーマット種別５１は、登録番号５３あるいは登録番号認証子５２の一部が情報本体５４の一部と重ね合わさせて配置されているか否かを示すフラグである。例えば同図(B)のように重ね合わされている場合に「1」、同図(A)のように重ね合わされていない場合に「0」というように設定されている。また、フォーマット種別５１のビット長Ｐ、登録番号認証子５２のビット長Ｑ、登録番号５３のビット長Ｓ、および登録番号５３と情報本体５４の重ね合ったビット長Ｖは固定長であり、これらの情報は端末装置２の制御手段５に格納管理されている。なお、ビット長Ｕは情報本体５４の内容によって変化する可変長である。

【００３４】同図(B)のようなフォーマットを使用する場合には情報管理センタ１において、まず情報本体の先頭からＶビットを取り出し、これを登録番号の最後のVビットに割り当てる。そして新たな登録番号がすでに登録されている他の登録番号と同じにならないように、残りの(S-V)ビットを設定する。

$$Vn = F(Ks, N)$$

【００３９】

$$Vn = F(Ks, H(N))$$

【００４０】以上の処理を行うことにより、図６に示した配布データを作成することができる。次に、利用者が購入したデジタル情報を利用する場合について説明する。利用者が端末装置２の入力手段８を使用して端末装置２の制御手段５に所定の指示を与えると、図８に示すフローチャートに添った処理が行なわれる。

【００４１】利用者はまず、端末装置２の入力手段８を使用して利用するデジタル情報を選択する(ステップS21)。この選択情報が供給される制御手段５は選択されたデジタル情報のフォーマット種別５１、登録番号認証子５２、登録番号５３をデジタル情報格納手段６から読み出す(ステップS22)。そして、フォーマット種別５１の判別をおこなう(ステップS23)。このフォーマット種別５１のデータが「０」の場合には(ステップS23→NO)、登録番号と情報本体の重ね合わせがないフォーマット（図６（A）参照）であるので、そのままステップS25に進む。フォーマット種別５１のデータが「１」の場合には（ステップS23→YES)、登録番号と情報本体の重ね合わせのあるフォーマット（図６（B）参照）であるので、ファイル読み出し位置をＶビットだけ戻す（ステップS24）。更に情報本体を読み出す（ステップS25）。そして、登録番号５３、登録番号認証子５２を情報管理センタ１に送信する（ステップS26）。

【００４２】情報管理センタ１の認証処理手段１０４では、受信した登録番号(Nr)５３と登録番号認証子(Vr)５２に対して以下のような処理を行い、登録番号５３が不正に変更されていないかのチェックを行う(ステップS27)。配布データ作成時に(1)式を使った場合は、セレクタ８５をｆ側に設定して入力端子に受信した登録番号Nrを与え、暗号関数演算部８３によって暗号化関数Fを用いて(3)式の計算を行い、出力Voを得る。また配布データ作成時に(2)式を使った場合は、セレクタ８５をe側に設定して入力端子に受信した登録番号Nrを与え、暗号関数演算部８３によって暗号化関数Ｆを用いて(4)式の計

【００３５】次に、情報管理センタ１の認証処理手段１０４の構成を図７に示し、以下に説明する。デジタル情報販売者は、あらかじめ暗号鍵Ksを作成しておき、この認証処理手段１０４の暗号鍵格納部８１に格納してある。認証処理手段１０４は、暗号鍵格納部８１、暗号関数演算部８３、一方向性ハッシュ関数演算部８４、及びセレクタ８５とで構成されており、一方向性ハッシュ関数演算部８４は、入力端子から入力される任意の長さの入力データXから短い固定長のデータH(X)を演算出力するものである。そして、この演算出力H(X)から入力データXを計算するのは極めて困難であり、また複数の異なったXから同一のH(X)の値が得られる確率が極めて小さいことを特徴とする演算部である。

【００３６】暗号関数演算部８３は、暗号鍵Ksとある決められた暗号化関数F()を使って入力データＹを暗号化する機能を持つ。ここで、暗号鍵Ksはデジタル情報販売者のみが知り、利用者（端末装置２）には知らせない情報である。したがって、F(Ks, Y)はデジタル情報販売者（情報管理センタ１）のみが計算することができる。逆に言えば、F(Ks, Y)が正しく計算されていれば、デジタル情報販売者が計算したということになり、F(Ks, Y)は認証子としての機能を持つことになる。

【００３７】登録番号認証子Vnは、セレクタ８５をｆ側に設定し、登録番号Nを入力端子に与えて、(1)式の演算による暗号化を行うか、あるいはセレクタ８５をe側に設定し、登録番号Nを入力端子に与えて一方向性ハッシュ関数演算部８４にて得た値(H(N))に対して暗号化を行うことにより作成される。この後者の場合は、(2)式の演算を行うことになる。

【００３８】

$$\cdots(1)式$$

$$\cdots(2)式$$

算を行い、出力Voを得る。

Vo = F(Ks, Nr)

【００４４】

Vo = F(Ks, H(Nr))

【００４５】そして、登録番号認証子Vrと出力Voが一致するかチェックする。Vr≠Voであれば(ステップS27→NO)、登録番号５３が不正に変更されていることになるので、使用禁止を意味するデータを端末装置２に送信する(ステップS28)。また、Vr＝Voであれば(ステップS27→YES)、登録番号５３は不正に変更されてないと判定できるので、ステップS29に進む。ステップS29では、登録番号Nrが使用条件テーブルに登録されているかのチェックを行う。もし登録されていなければ(ステップS29→NO)、その登録番号Nrは偽造されたものであると見なし、使用禁止を意味するデータを端末装置２に送信する（ステップS28）。

【００４６】そして、登録番号Nrが使用条件テーブルに登録されている場合は（ステップS29→YES）、さらに、期間制限フラグが「1」にセットされているか否かをチェックする(ステップS30)。期間制限フラグが「0」の場合は（ステップS30→NO）、特に期間制限が設定されていないので、そのままステップS32へ進む。期間制限フラグが「1」にセットされている場合には（ステップS30→YES）、現在日時が許可開始日時と許可終了日時との間にあることを確認する(ステップS31)。そして、現在日時が許可開始日時と許可終了日時との間にある場合には（ステップS31→YES）、ステップS32へ進む。

【００４７】このステップS31において、（期間制限フラグが「1」であり、）許可開始日時あるいは許可終了日時が所定の初期値である場合は、初期値である項目に関し許可条件を満たすと見なす。すなわち、許可開始日時が初期値であれば、許可終了日時のみチェックし、現在日時が許可終了日時以前であればステップS32へ進む。同様に、許可終了日が初期値であれば、許可開始日時のみチェックし、現在日時が許可開始日時以降であればステップS32へ進む。また、許可期間内でなければ（ステップS31→NO）、ステップS28に進み、使用禁止を意味するデータを端末装置２に送信する。

【００４８】ステップS32では回数制限フラグが「1」にセットされているかチェックする。回数制限フラグが「0」の場合は（ステップS32→NO）、特に使用回数の制限がないのでそのままステップS35に進む。回数制限フラグが「1」にセットされている場合は（ステップS32→YES）、使用可能回数が「0」より大きいかをチェックする(ステップS33)。そして、使用可能回数が「0」の場合は（ステップS33→NO）、ステップS28に進み、使用禁止を意味するデータを端末装置２に送信する。使用可能回数が「0」でない場合には、その使用可能回数を1だけ減じ(ステップS34)、ステップS35へ進む。そして、以上の判定により、正当な使用であると確認された場合には使

【００４３】

・・・(3)式

・・・(4)式

用許可を意味するデータを端末装置２に送信する(ステップS35)。

【００４９】端末装置２の制御手段５は、通信回線３及び通信手段４を介して情報管理センタ１から受け取ったデータが使用許可であるか否かをチェックして(ステップS36)、使用許可であれば（ステップS36→YES）、デジタル情報本体をデジタル情報格納手段６から読みだしてデジタル情報のフォーマットに従った処理を行い、ディスプレイ、スピーカ等の出力手段９に出力する(ステップS37)。また、情報管理センタ１から受け取ったデータが使用禁止であれば、その旨のエラーメッセージを出力手段９に出力し処理を終了する(ステップS38)。このように処理を行うことにより、正規に登録し、使用期間、回数制限を守っている正当な端末装置（利用者）にだけ、デジタル情報の使用許可を与えることができる。

【００５０】

【発明の効果】本発明のデジタル情報管理システム及びデジタル情報管理方法は、単にデジタル情報の不正コピーを防止するだけでなく、使用期間、使用回数、あるいはその両方を限定してデジタル情報を利用させることが可能となる。厳密には、デジタル情報のコピー行為そのものは可能であるが、使用回数を制限した場合には、デジタル情報を正当な方法で入手した利用者が別の利用者にデジタル情報のコピーを渡しても、コピーを入手した別の利用者が使用した回数だけ元の利用者の使用できる回数が減ってしまうので、元の利用者が不利益を被るので、このような行為（デジタル情報のコピー）を十分抑制できる。

【００５１】また、正当な利用者が、例えば自宅と仕事場の２個所でデジタル情報を使用したい場合には、別々の端末装置にデジタル情報をコピーして、それぞれの端末装置で、正当に利用することができる。この場合でも、使用回数が制限されている場合には、それぞれの端末装置で使用された回数の合計で使用回数の制限が行われるので、情報提供者が被害を受けることはない。さらに、デジタル情報の使用条件や使用状況を全て情報管理センタで記録管理するので、端末装置の利用者がこれらの情報を不正に変更することは非常に困難となる。

【００５２】一方、利用者にとっては、個別のニーズに応じて使用期間や使用回数を細かく設定した購入ができるので、これらの条件を設定しない売り切りの場合よりも無駄がなく、実質的に安い料金で必要な情報を必要なだけ利用することができる。また、デジタル情報を端末装置に格納して使用許可情報だけを端末装置に送信する方式なので、端末装置にデジタル情報を蓄積せず利用の度にセンタからダウンロードする従来の方式と比べて、

通信コストが安く済み、利用する際の待ち時間も少なくなるという優れた効果がある。

【００５３】また本発明では、デジタル情報本体に固有の登録番号と登録番号認証子が情報管理センタにより付与されており、情報センタだけが知る暗号鍵がないと登録番号認証子は作成できないので、利用者が登録番号を偽造して不正にデジタル情報を使うことは非常に困難である。

【００５４】さらに本発明は、端末装置内に暗号処理機能を必要とせず、端末装置内に暗号鍵を格納していない。すなわち端末装置に複雑な処理処理機能や機密性を要求される部分がない。従って端末装置に特殊な装置を付加することなく、一般的な構成のコンピュータを端末装置として構成することができるので、端末装置のコストが従来より安くなると同時に、より多くのユーザが利用可能となる。また、一般的な構成のコンピュータを端末装置として構成することができることにより、デジタル情報を利用する端末装置の種類が限定されないので、利用者はデジタル情報を複数の異なった端末装置からでも利用することができ、利用者の利便性が向上するという効果がある。

【００５５】さらに、登録番号あるいは登録番号認証子の一部のビット列と情報本体の一部のビット列を一致させ、その一致部分を端末装置内で重ね合わせて格納することにより、端末装置で行われる不正な改変にも対応することができる。

【図面の簡単な説明】

【図１】本発明のデジタル情報管理システムの一実施例を示す構成図である。

【図２】本発明のデジタル情報管理システムの端末装置例を示す構成図である。

【図３】情報管理センタを示す構成図である。

【図４】使用条件テーブルを説明するための図である。

【図５】使用条件テーブルの設定方法を説明するフローチャート図である。

【図６】端末装置に供給するデータフォーマットの例を示す構成図である。

【図７】本発明の情報処理センタの認証処理手段の例を示す構成図である。

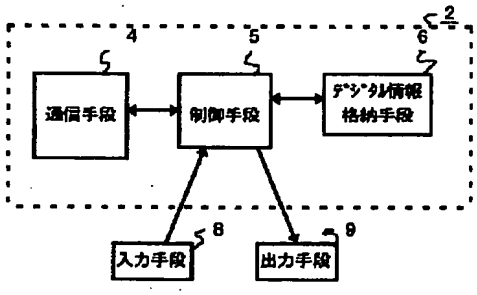
【図８】デジタル情報の利用手順を説明するためのフローチャート図である。

【符号の説明】

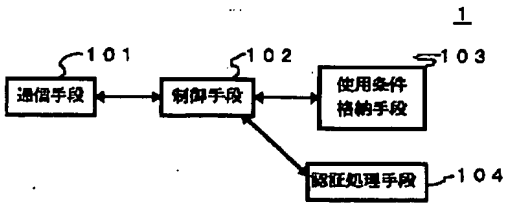
１　情報管理センタ
２　端末装置
３　通信回線
４　通信手段（第１の通信手段）
５　制御手段（第１の制御手段）
６　デジタル情報格納手段
８　入力手段
９　出力手段
１０１　通信手段（第２の通信手段）
１０２　制御手段（第２の制御手段）
１０３　使用条件格納手段
１０４　認証処理手段

【図１】

【図２】



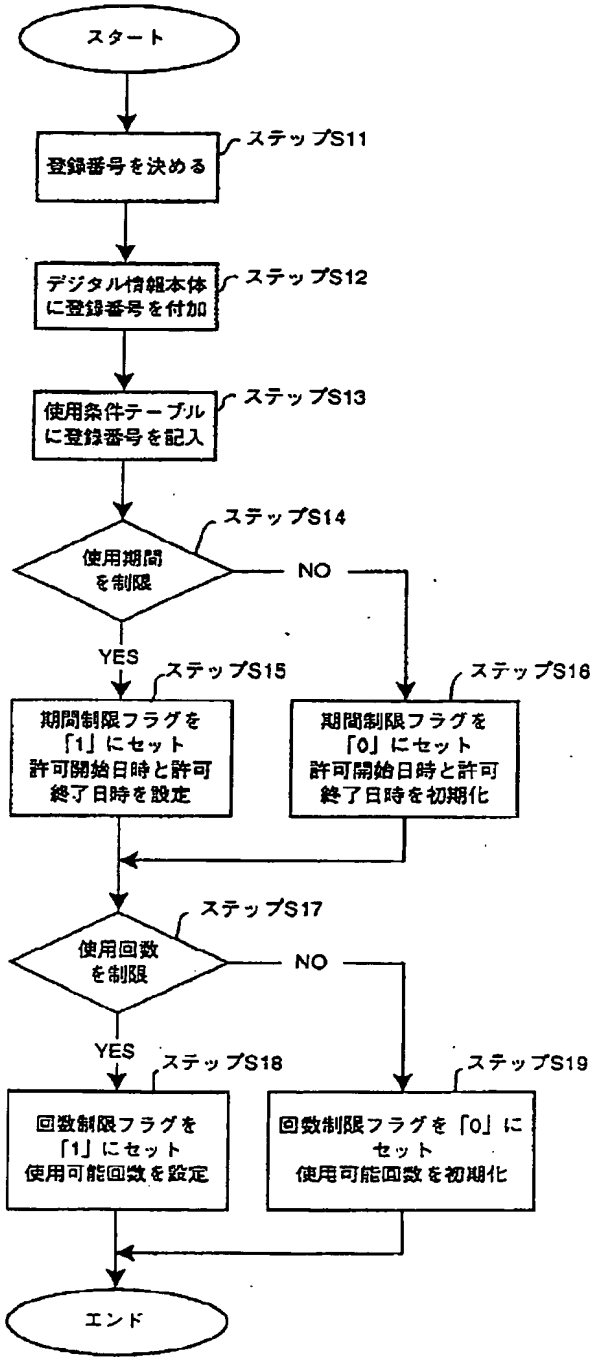
【図３】



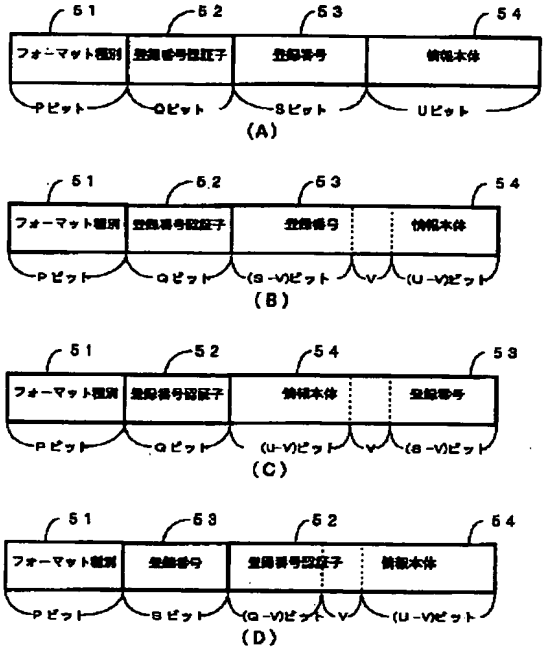
【図４】

登録番号	期間制限ﾌﾗｸﾞ	回数制限ﾌﾗｸﾞ	許可開始日時	許可終了日時	使用回数
N	0	1	0	0	3

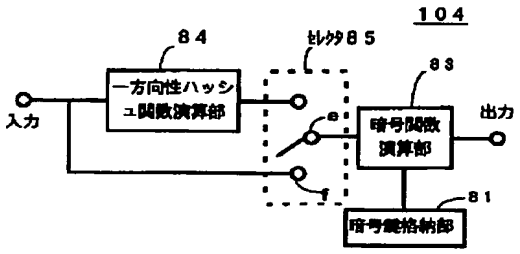
【図５】


スタート
登録番号を決める
ステップS11
デジタル情報本体に登録番号を付加
ステップS12
使用条件テーブルに登録番号を記入
ステップS13
使用期間を制限
ステップS14
NO
YES
期間制限フラグを「1」にセット 許可開始日時と許可終了日時を設定
ステップS15
期間制限フラグを「0」にセット 許可開始日時と許可終了日時を初期化
ステップS16
使用回数を制限
ステップS17
NO
YES
回数制限フラグを「1」にセット 使用可能回数を設定
ステップS18
回数制限フラグを「0」にセット 使用可能回数を初期化
ステップS19
エンド

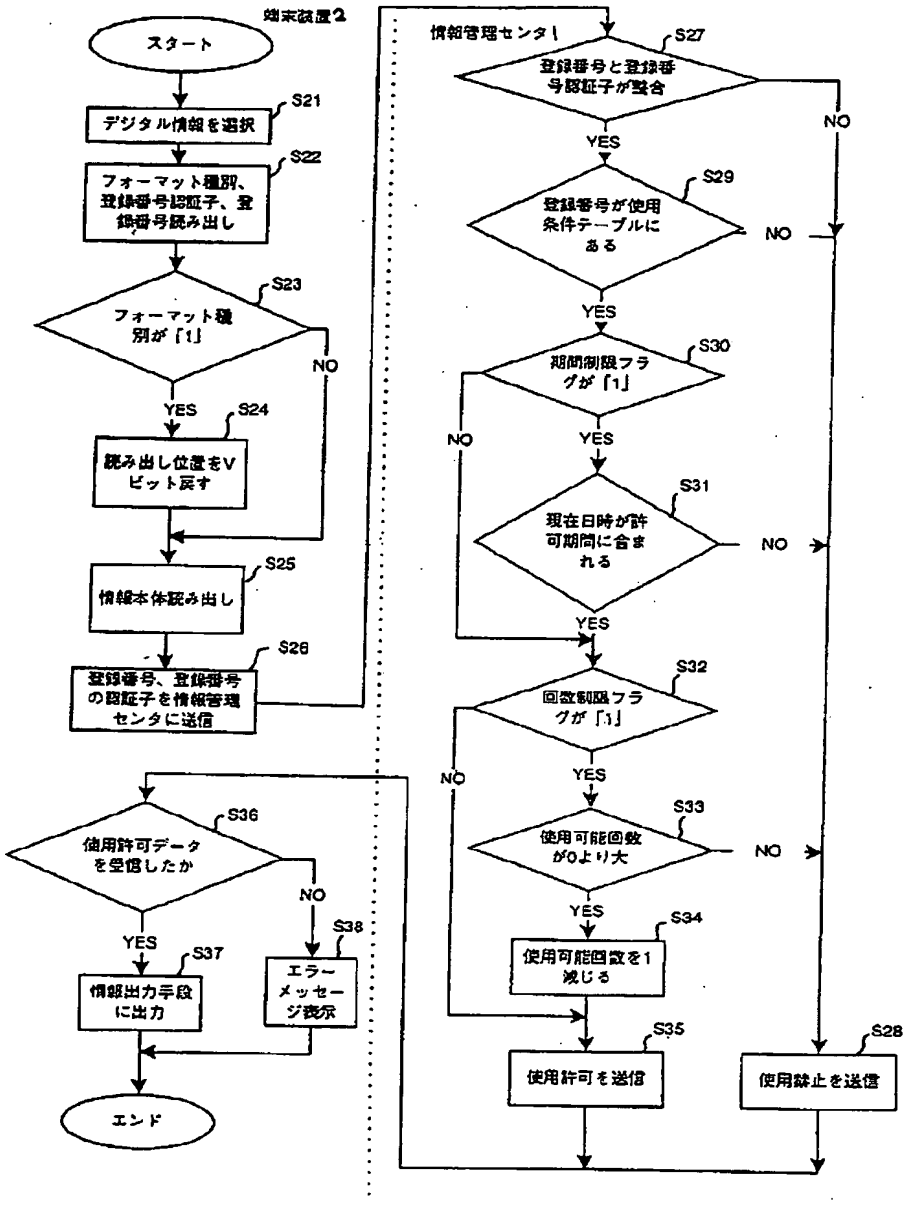
【図６】


51
52
53
54
フォーマット種別
登録番号識別子
登録番号
情報本体
Pビット
Qビット
Sビット
Uビット
(A)
(S-V)ビット
V
(U-V)ビット
(B)
(U-V)ビット
(C)
(D)

【図７】


104
84
セレクタ85
83
一方向性ハッシュ関数演算部
入力
暗号関数演算部
出力
81
暗号鍵格納部

【図８】


端末装置2
スタート
S21
デジタル情報を選択
S22
フォーマット種別、登録番号認証子、登録番号読み出し
S23
フォーマット種別が「1」
NO
YES
S24
読み出し位置をVビット戻す
S25
情報本体読み出し
S26
登録番号、登録番号の認証子を情報管理センタに送信
S36
使用許可データを受信したか
NO
YES
S37
情報出力手段に出力
S38
エラーメッセージ表示
エンド
情報管理センタ1
S27
登録番号と登録番号認証子が整合
NO
YES
S29
登録番号が使用条件テーブルにある
NO
YES
S30
期間制限フラグが「1」
NO
YES
S31
現在日時が許可期間に含まれる
NO
YES
S32
回数制限フラグが「1」
NO
YES
S33
使用可能回数が0より大
NO
YES
S34
使用可能回数を1減じる
S35
使用許可を送信
S28
使用禁止を送信